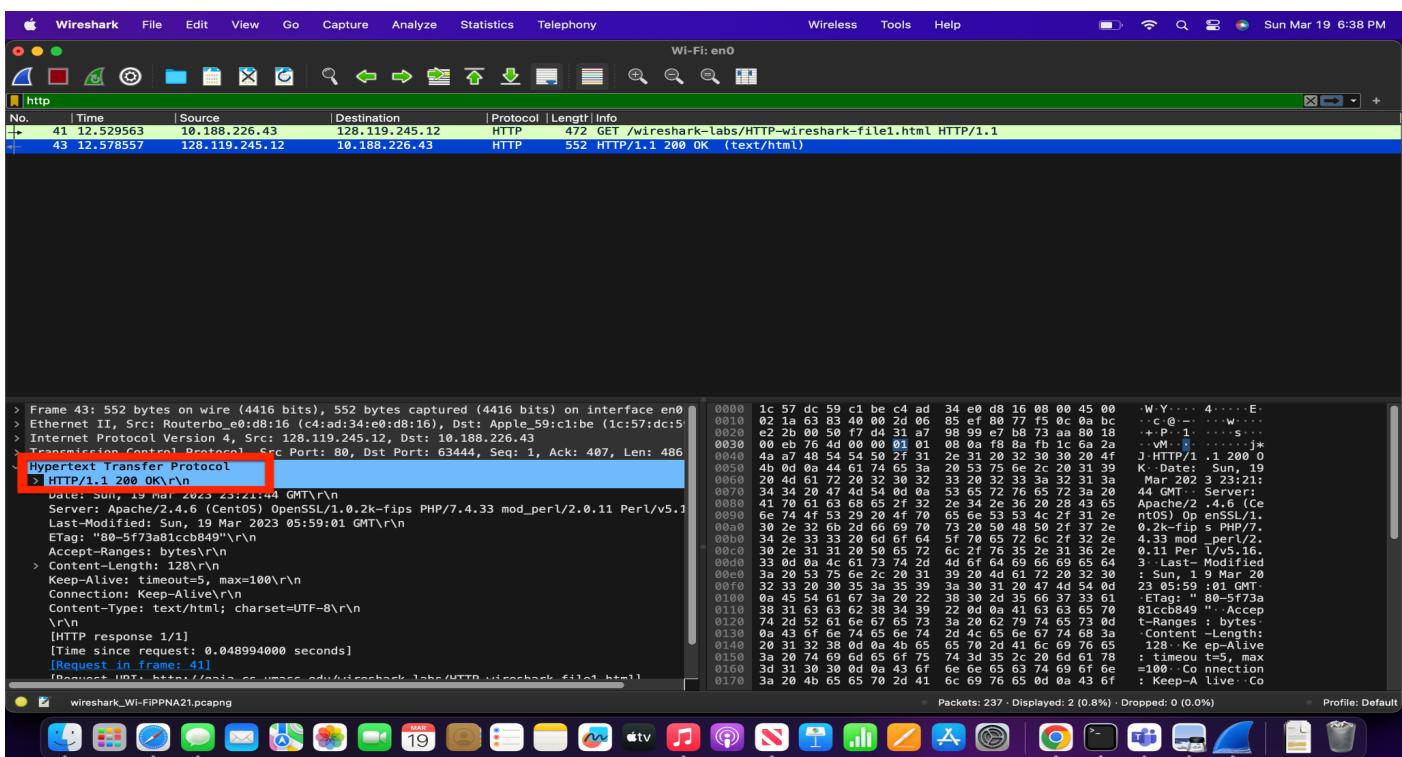
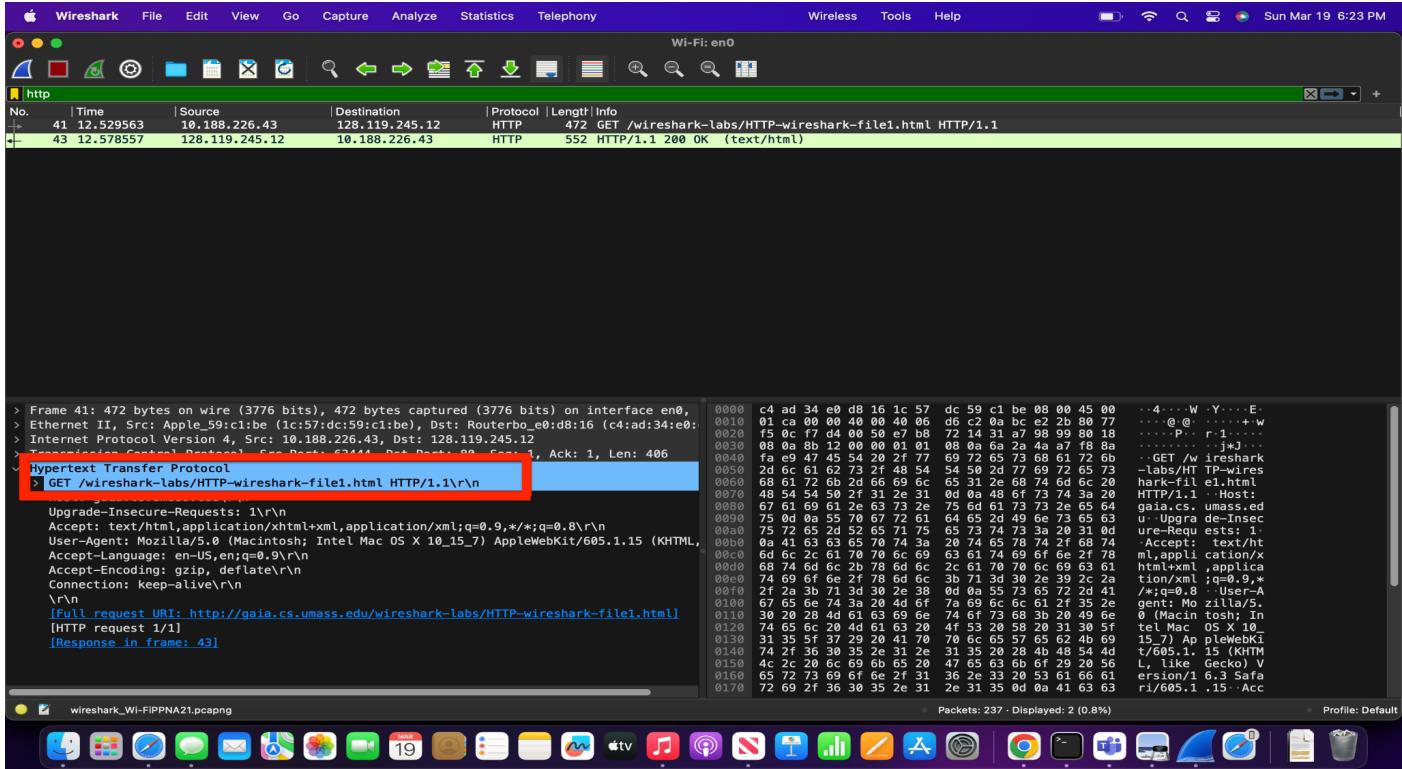


Name: Ayushi Patel  
 CSE 5344 : Computer Networks  
 Project 2

## The Basic HTTP GET Response Interaction

- Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
  - The browser is running HTTP version 1.1 and the server is running HTTP version 1.1.



## 2. What languages (if any) does your browser indicate that it can accept to the server?

- The browser can accept 'en-US'

Frame 41: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface en0  
 Ethernet II, Src: Apple\_59:c1:be (1c:57:dc:59:c1:be), Dst: Router0\_e0:d8:16 (c4:ad:34:e0:  
 Internet Protocol Version 4, Src: 10.188.226.43, Dst: 128.119.245.12  
 Transmission Control Protocol, Src Port: 63444, Dst Port: 80, Seq: 1, Ack: 1, Len: 406  
 Hypertext Transfer Protocol  
 > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 Upgrade-Insecure-Requests: 1\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.2 Safari/605.1.15\r
 Accept-Language: en-US,en;q=0.9\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
 [HTTP request 1/1]
 [Response in frame: 43]

0060 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 6d 6c 20 hark-fil e1.html
 0070 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 · Host:
 0080 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 u: Upgra de-Insec
 0090 75 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 ure-Requ ests: 1-
 00a0 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d
 00b0 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74
 00c0 6d 6c 2d 61 70 78 6c 69 63 61 74 69 6f 6e 2f 78 Accept: text/ht
 00d0 68 74 6d 6c 2b 78 6d 6e 2d 61 70 78 6c 69 63 61 ml,application/x
 00e0 74 69 61 66 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a html+xml , applica
 00f0 2f 2a 3f 71 3d 30 2e 38 0d 0a 48 6f 73 74 3a 20 41 tion/xml ;q=0.9,\*
 0100 67 65 68 74 39 20 6d 61 70 6c 69 6f 6e 2f 78 56 /\*;q=0.8 -User-A
 0110 67 65 68 74 39 20 6d 61 70 6c 69 6f 6e 2f 78 56 gent: Mozilla/5.
 0120 74 65 7c 2d 4d 61 63 66 4f 53 2d 58 20 31 30 5f 74 65 7c 2d 4d 61 63 66 4f 53 2d 58 20 31 30 5f tel Mac OS X 10
 0130 31 35 5f 37 29 20 41 70 70 6c 65 57 65 62 4b 69 15.7 Ap webk i
 0140 74 2f 36 38 35 2e 31 2e 31 35 20 28 4b 48 54 4d t/605.1.15 (KHTML
 0150 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 29 56 L, like Gecko) V
 0160 65 72 73 69 6f 6e 2f 31 36 2e 33 20 53 61 66 61 ersion/12.1.2 Safa
 0170 72 69 2f 36 30 35 2e 31 2e 31 35 0d 0a 41 63 63 ri/605.1.15 · Acc
 0180 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e ept-Language: en
 0190 2d 55 2c 65 6c 3b 71 3d 30 2e 39 0d 0a 41 63 -US,en;q=0.9 · Ac
 01a0 63 65 70 74 2d 45 6e 63 6f 64 69 66 67 3a 20 67 cept-Encoding: g
 01b0 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f zip, def late: Co
 01c0 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
 01d0 6c 69 76 65 0d 0a 0d 0a live....

## 3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

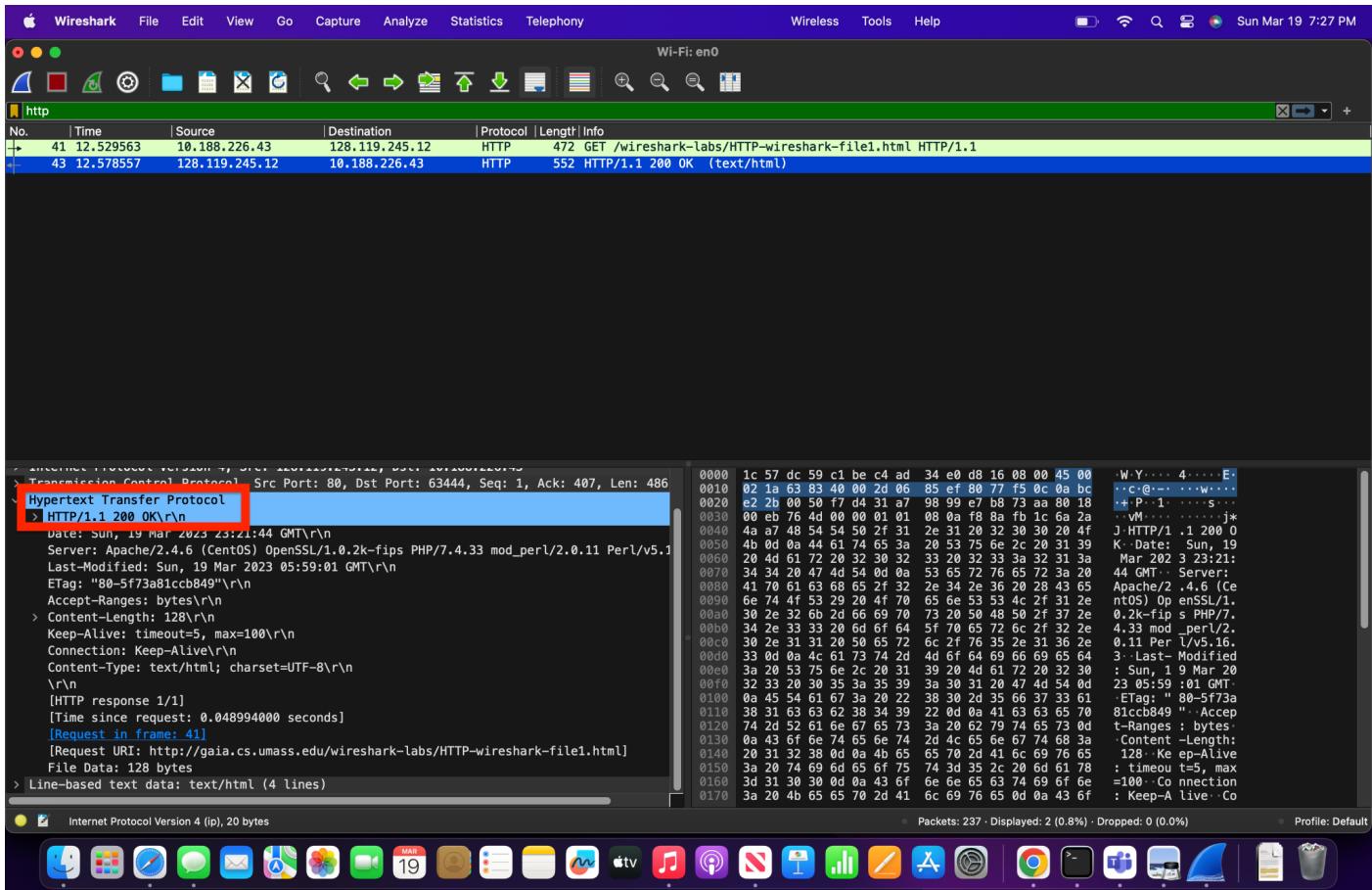
- IP address of my computer: 10.188.226.43 and IP address of server: 128.119.245.12

Frame 41: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface en0  
 Ethernet II, Src: Apple\_59:c1:be (1c:57:dc:59:c1:be), Dst: Router0\_e0:d8:16 (c4:ad:34:e0:  
 Internet Protocol Version 4, Src: 10.188.226.43, Dst: 128.119.245.12  
 Transmission Control Protocol, Src Port: 63444, Dst Port: 80, Seq: 1, Ack: 1, Len: 406  
 Hypertext Transfer Protocol  
 > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 Upgrade-Insecure-Requests: 1\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n
 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.2 Safari/605.1.15\r
 Accept-Language: en-US,en;q=0.9\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
 [HTTP request 1/1]
 [Response in frame: 43]

0000 c4 ad 34 e0 d8 16 1c 57 dc 59 c1 b1 ee 08 00 45 00 hark-fil e1.html
 0010 01 c0 00 00 40 00 40 00 06 d6 c2 0a bc e2 2b 80 77 HTTP/1.1 · Host:
 0020 f5 0c f7 d4 00 50 00 e7 b8 72 14 31 a7 98 99 80 18 u: Upgra de-Insec
 0030 08 0a 8b 12 00 00 01 01 08 0a 6a 2a 4a a7 f8 8a ure-Requ ests: 1-
 0040 fa e9 47 45 54 20 2f 77 69 62 65 73 68 61 72 6b
 0050 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73
 0060 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 6d 6c 20
 0070 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20
 0080 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64
 0090 75 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63
 00a0 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d
 00b0 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74
 00c0 6d 6c 2d 61 70 6c 69 63 61 74 69 6f 6e 2f 78
 00d0 68 74 6d 6c 2b 78 6d 6e 2d 61 70 78 6c 69 63 61
 00e0 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a
 00f0 2f 2a 3f 71 3d 30 2e 38 0d 0a 48 6f 73 74 3a 20 41
 0100 67 65 68 74 3a 20 6d 61 70 6c 69 6f 6e 2f 78 56
 0110 30 2d 2b 6c 69 6f 6e 2f 78 6d 65 73 74 3a 20 49 6e
 0120 74 65 7c 2d 4d 61 63 66 4f 53 2d 58 20 31 30 5f
 0130 31 35 5f 37 29 20 41 70 6c 65 57 65 62 4b 69 15.7 Ap webk i
 0140 74 2f 36 38 35 2e 31 2e 31 35 20 28 4b 48 54 4d t/605.1.15 (KHTML
 0150 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 29 56 L, like Gecko) V
 0160 65 72 73 69 6f 6e 2f 31 36 2e 33 20 53 61 66 61 ersion/12.1.2 Safa
 0170 72 69 2f 36 30 35 2e 31 2e 31 35 0d 0a 41 63 63 ri/605.1.15 · Acc
 0180 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e ept-Language: en
 0190 2d 55 2c 65 6c 3b 71 3d 30 2e 39 0d 0a 41 63 -US,en;q=0.9 · Ac
 01a0 63 65 70 74 2d 45 6e 63 6f 64 69 66 67 3a 20 67 cept-Encoding: g
 01b0 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f zip, def late: Co
 01c0 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
 01d0 6c 69 76 65 0d 0a 0d 0a live....

#### 4. What is the status code returned from the server to your browser?

- The status code returned from the server to browser is : 200 OK



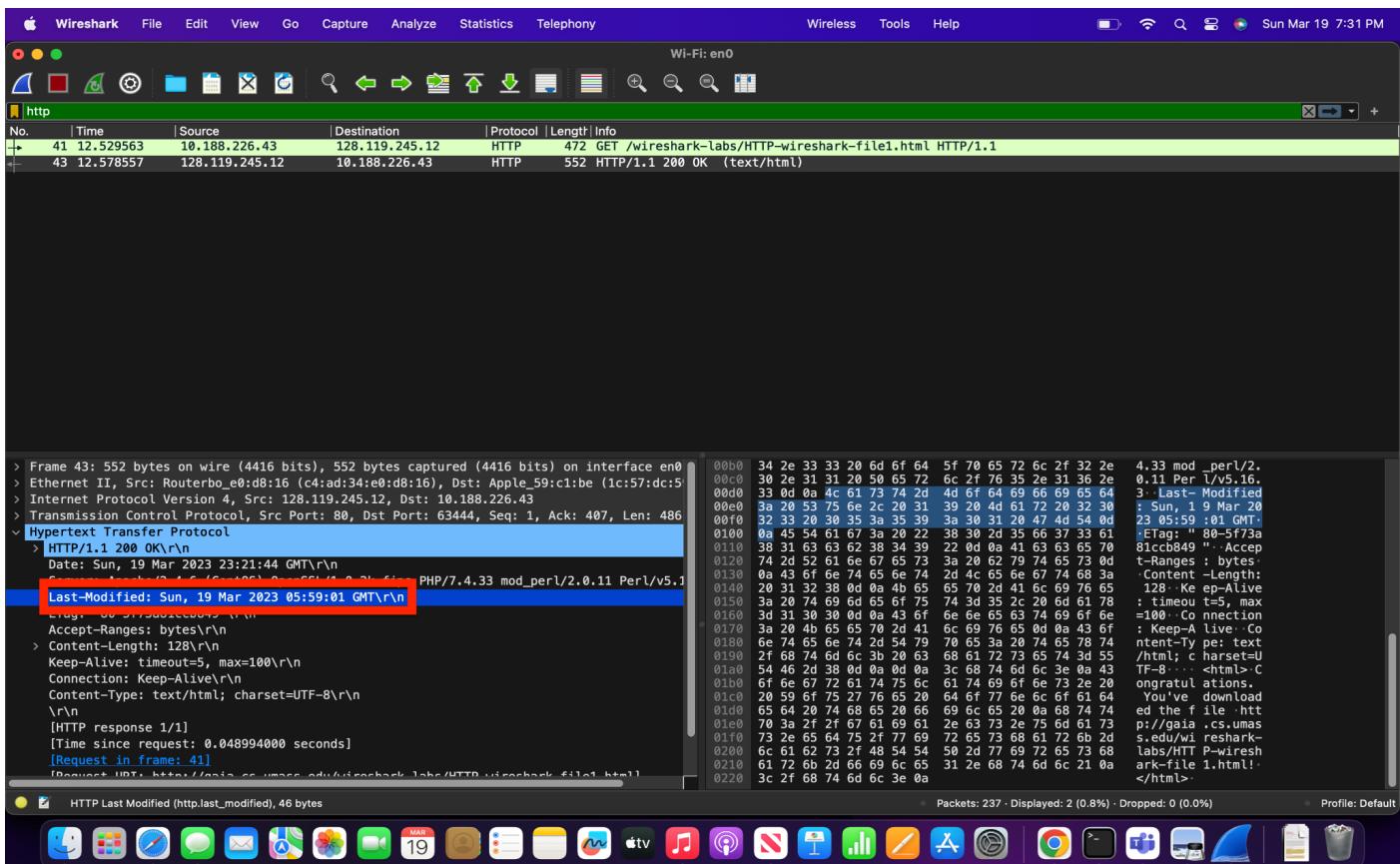
Wireshark screenshot showing an HTTP session. The request (41) is from 12.52.95.63 to 128.119.245.12. The response (43) is from 128.119.245.12 to 10.188.226.43, containing the HTML content of 'HTTP-wireshark-file1.html'. The status line 'HTTP/1.1 200 OK\r\n' is highlighted in red.

HTTP Response Body:

```
Date: Sun, 19 Mar 2023 23:21:44 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.1Last-Modified: Sun, 19 Mar 2023 05:59:01 GMT\r\nETag: "80-5f73a81ccb849"\r\nAccept-Ranges: bytes\r\nContent-Length: 128\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1]\r\n[Time since request: 0.048994000 seconds]\r\n[Request in frame: 41]\r\n[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]\r\nFile Data: 128 bytes\r\nLine-based text data: text/html (4 lines)
```

#### 5. When was the HTML file that you are retrieving last modified at the server?

- The HTML file was last modified on Sun, 19 Mar 2023 05:59:01 GMT



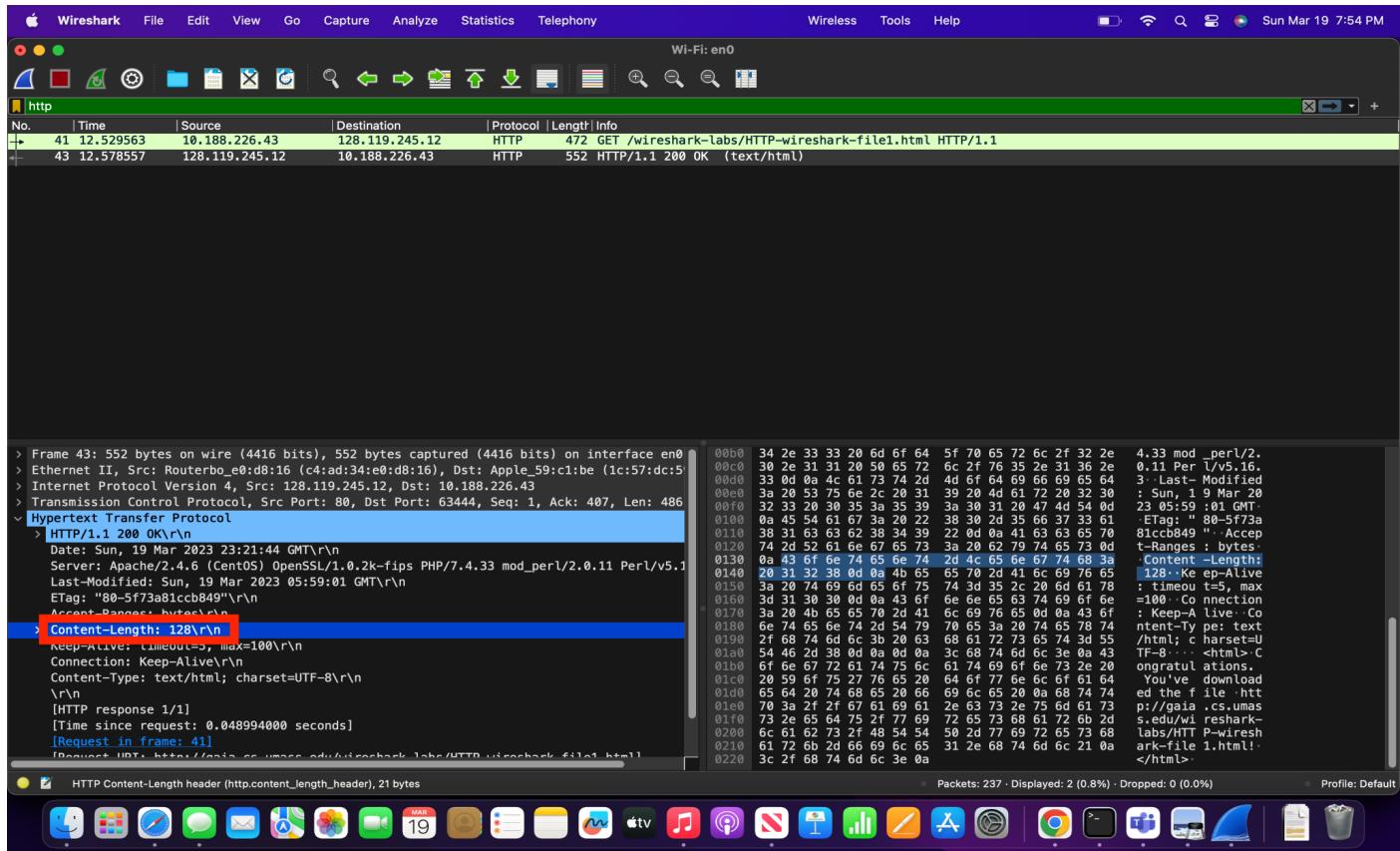
Wireshark screenshot showing an HTTP session. The request (41) is from 12.52.95.63 to 128.119.245.12. The response (43) is from 128.119.245.12 to 10.188.226.43, containing the HTML content of 'HTTP-wireshark-file1.html'. The 'Last-Modified' header value 'Sun, 19 Mar 2023 05:59:01 GMT\r\n' is highlighted in red.

HTTP Response Body:

```
Last-Modified: Sun, 19 Mar 2023 05:59:01 GMT\r\nDate: Sun, 19 Mar 2023 23:21:44 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.1Content-Type: text/html; charset=UTF-8\r\nContent-Length: 128\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\n\r\n[HTTP response 1/1]\r\n[Time since request: 0.048994000 seconds]\r\n[Request in frame: 41]\r\n[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]\r\nFile Data: 128 bytes\r\nLine-based text data: text/html (4 lines)
```

6. How many bytes of content are being returned to your browser?

- 128 bytes are being returned to the browser.



7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

- No, all of the headers can be found in the raw data.

## The HTTP CONDITIONAL GET Response Interaction

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
- No, there is no “IF-MODIFIED-SINCE” line in the first HTTP GET.

Wireshark screenshot showing the first HTTP GET request from the browser to the server. The request is for /wireshark-labs/HTTP-wireshark-file2.html. The response shows a 200 OK status with the file content.

Protocol Version: 4, Src Port: 58256, Dst Port: 80, Seq: 1, Ack: 1, Len: 478

Transmission Control Protocol, Src Port: 58256, Dst Port: 80, Seq: 1, Ack: 1, Len: 478

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file2.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.122 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

[HTTP request 1/2]

[Response in frame: 1829]

[Next request in frame: 1837]

HTTP Accept Language (http.accept\_language), 33 bytes

Packets: 1898 - Displayed: 4 (0.2%) - Dropped: 0 (0.0%) - Profile: Default

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

- Yes because we can see the contents in the Line-based text data field.

Wireshark screenshot showing the first HTTP GET request from the browser to the server. The request is for /wireshark-labs/HTTP-wireshark-file2.html. The response shows a 200 OK status with the file content.

Protocol Version: 4, Src Port: 58256, Dst Port: 80, Seq: 1, Ack: 1, Len: 478

Transmission Control Protocol, Src Port: 58256, Dst Port: 80, Seq: 1, Ack: 1, Len: 478

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file2.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.122 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

[HTTP request 1/2]

[Response in frame: 1825]

[Next request in frame: 1837]

Line-based text data: text/html (10 lines)

\n<html>\n\nCongratulations again! Now you've downloaded the file lab2-2.html. <br>\nThis file's last modification date will not change. <p>\nThus if you download this multiple times on your browser, a complete copy <br>\nwill only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\nfield in your browser's HTTP GET request to the server.\n\n</html>\n

Packets: 1898 - Displayed: 4 (0.2%) - Dropped: 0 (0.0%) - Profile: Default

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

- Yes, there is an “IF-MODIFIED-SINCE” line in the second HTTP GET request. The information followed is: Sun, 19 Mar 2023 05:59:01 GMT which is the date of the last modification of the file from the previous get request.

The screenshot shows the Wireshark interface with several captured HTTP requests. The packet list pane shows the following sequence:

- Packet 1825: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
- Packet 1829: 796 HTTP/1.1 200 OK (text/html)
- Packet 1837: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
- Packet 1839: 305 HTTP/1.1 304 Not Modified

The packet details pane displays the raw HTTP request for the second GET request:

```

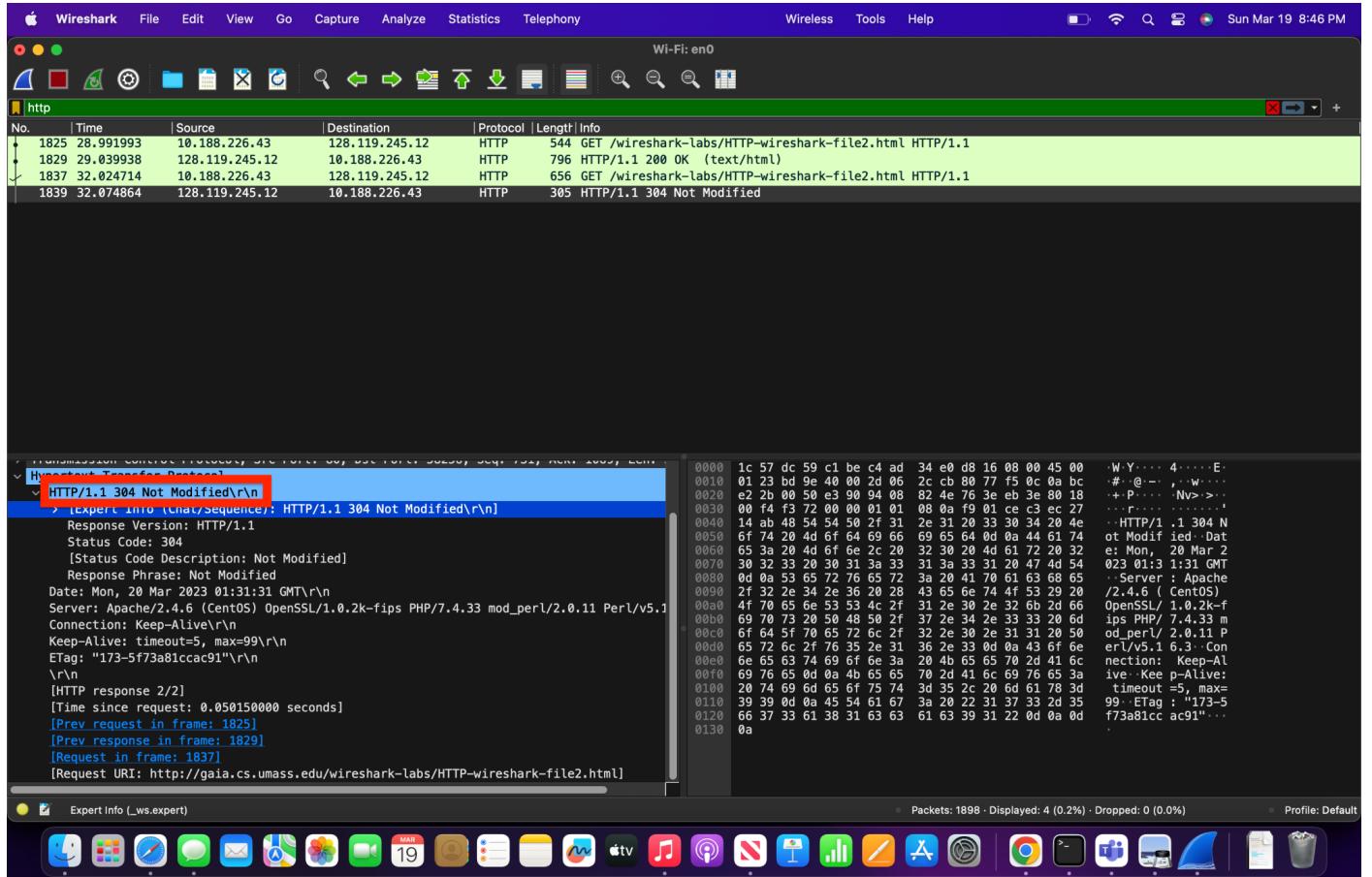
> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,in
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5f73a81ccac91"\r\n
If-Modified-Since: Sun, 19 Mar 2023 05:59:01 GMT\r\n

```

The "If-Modified-Since" header is highlighted in red. The packet bytes pane shows the raw hex and ASCII data for this request. The packet details pane also shows the response headers for the second request, including the "Last-Modified" and "Etag" fields.

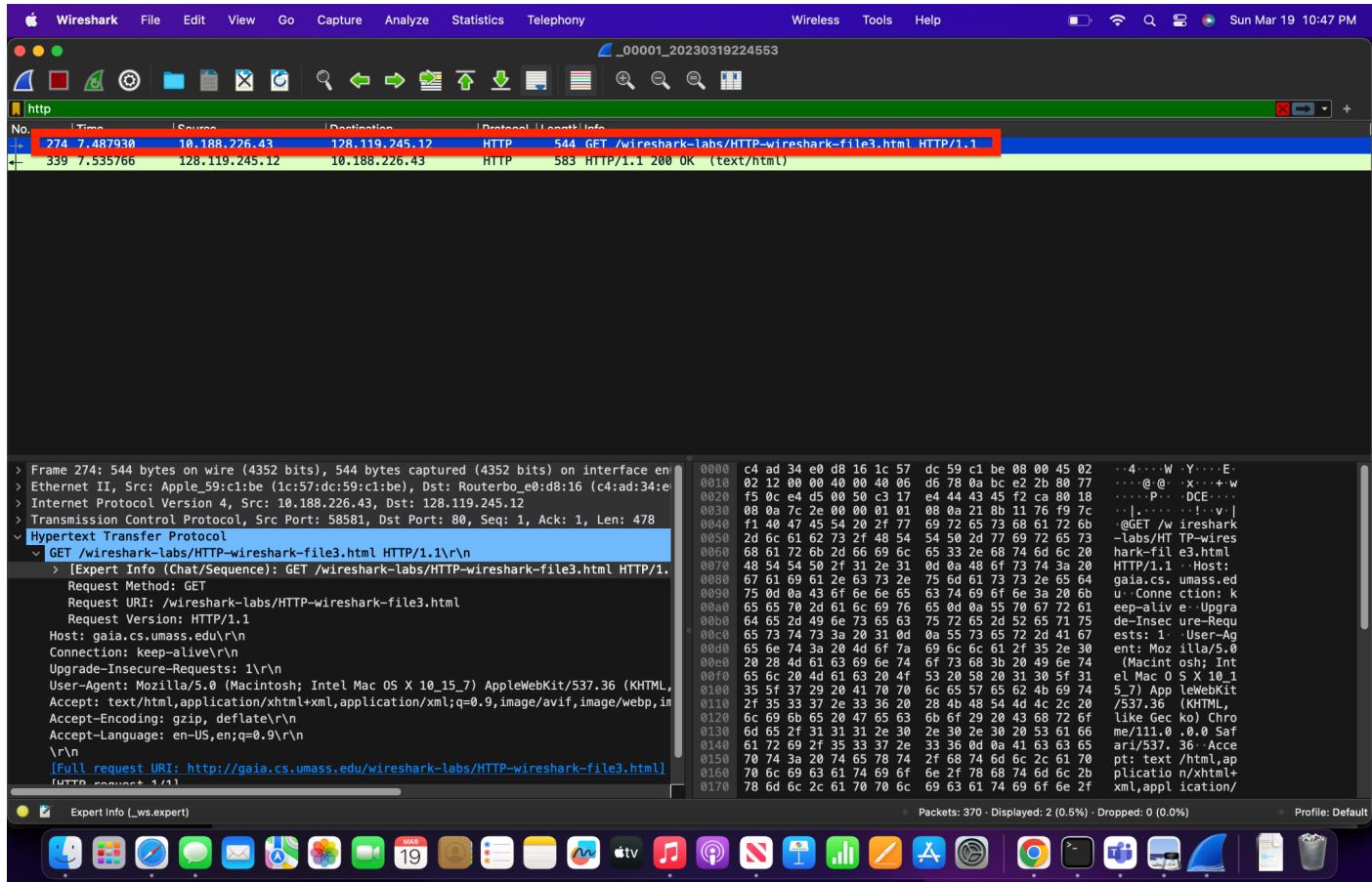
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

- The HTTP Status Code and phrases returned from the server in response to the second HTTP GET are “304” and “Not-Modified”. The server didn’t explicitly return the contents of the file since the browser loaded it from its cache.



## Retrieving Long Documents

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?
- The browser sent only one HTTP GET request message. Packet number 274 contains the HTTP GET message.



**13.** Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

- Packet number 335 in the trace contains the status code and phrase associated with the response to the HTTP GET request.

The screenshot shows a Wireshark capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Telephoney. The wireless tools and help options are also visible. The main pane displays two network frames. Frame 274 (HTTP GET) and Frame 339 (HTTP response). The response frame details show a status line: "HTTP/1.1 200 OK". Below this, the response body contains the text of the US Bill of Rights. The bottom status bar indicates 4,861 bytes of TCP segments and 370 packets displayed.

**14.** What is the status code and phrase in the response?

- The status code and phrase in response is '200 OK'.

This screenshot is identical to the one above, showing the same Wireshark interface and the same capture of the Bill of Rights document. The status code '200 OK' is again highlighted in the response details, and the response body shows the full text of the document.

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

- There were 4 data containing TCP segments containing 1448 ,1448 ,1448 and 517 bytes respectively for a total of 4861 bytes.

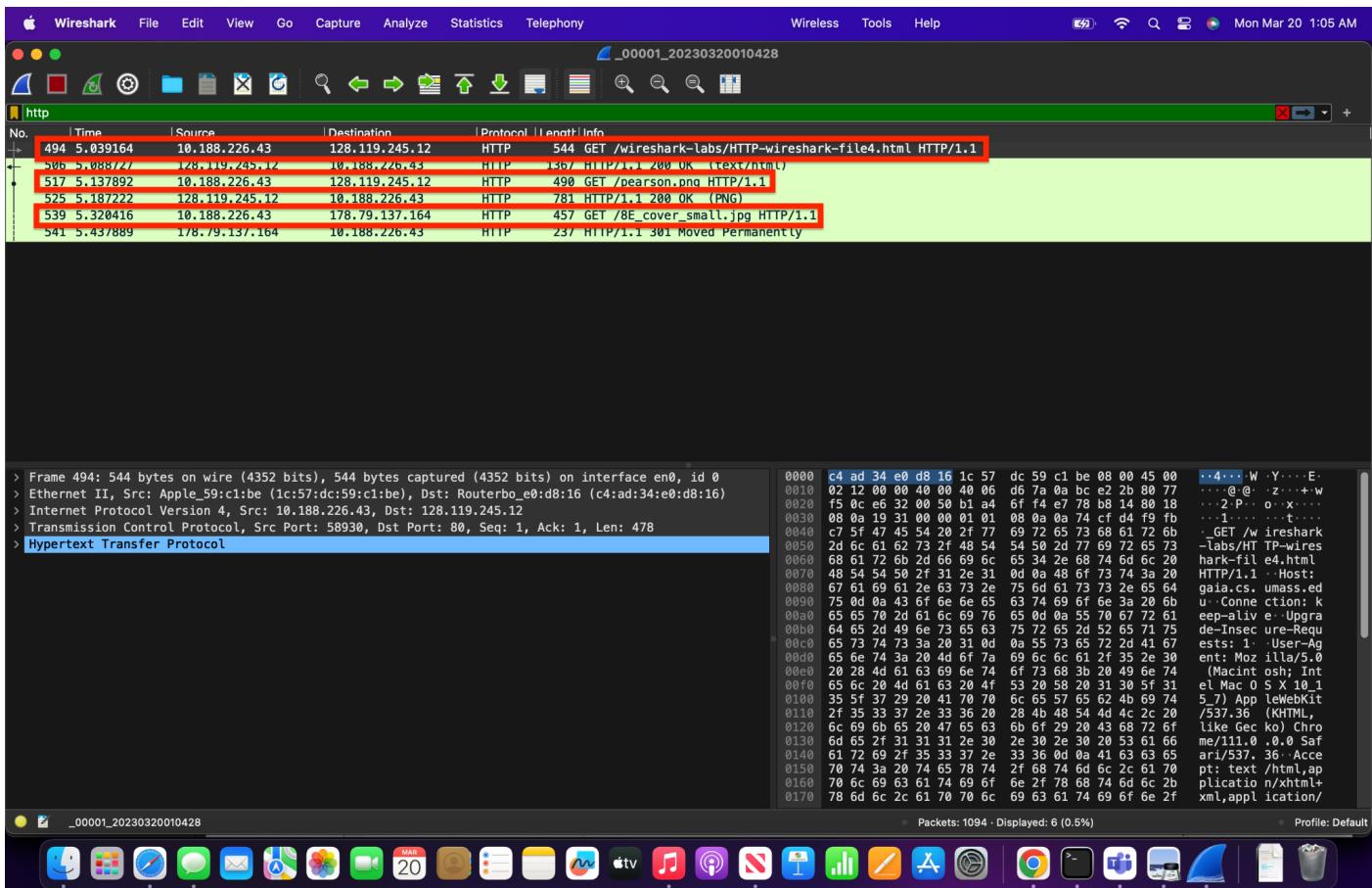
The screenshot shows the Wireshark interface with the following details:

- Panels:** Top: Menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephone, Wireless, Tools, Help), Status bar (Mon Mar 20 12:50 AM). Middle-left: Network traffic list (http), packet details (Frame 339), and bytes (Frame 339). Middle-right: Reassembled TCP Segments pane (4861 bytes).
- Network Traffic:** Two frames are visible:
  - Frame 274: 544 bytes on wire (436 bits), 544 bytes captured (436 bits) on interface en0, id 0. Details: Ethernet II, Src: Routerbo\_e0:d8:16 (c4:ad:34:e0:d8:16), Dst: Apple\_59:c1:be (1c:57:dc:59:c1:be). Protocol: HTTP. Info: GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  - Frame 339: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0. Details: Ethernet II, Src: Routerbo\_e0:d8:16 (c4:ad:34:e0:d8:16), Dst: Apple\_59:c1:be (1c:57:dc:59:c1:be). Protocol: HTTP. Info: HTTP/1.1 200 OK (text/html)
- Reassembled TCP Segments:** The pane displays the reassembled TCP segments (4861 bytes) from frame 339. It shows the HTML content of the Bill of Rights, including the title "THE BILL OF RIGHTS" and various sections of the document.
- Bottom:** A toolbar with icons for file operations, and a Mac OS X-style dock with various application icons.

## HTML Documents With Embedded Objects

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

- 3 HTTP GET request messages were sent by the browser to the server.
  - The 1st GET request was sent to retrieve the html(base file). This html file contains a link to 2 images.
  - So, the 2nd and 3rd requests were sent to retrieve those images.
- 1st IP Address: 128.119.245.12
- 2nd IP Address: 128.119.245.12
- 3rd IP Address: 178.79.137.164



17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

- We can determine whether our data were downloaded serially or in parallel by looking at the TCP ports. The two images in this particular case were received sequentially because they were sent over two separate TCP connections.

The screenshot shows a Wireshark capture window with the following details:

- Capturing from Wi-Fi: en0**
- http** selected in the tree view.
- Frame 1034: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface en0, id 0**
- Ethernet II, Src: Apple\_59:c1:be (1c:57:dc:59:c1:be), Dst: Routerbo\_e0:d8:16 (c4:ad:34:e0:d8:16)**
- Internet Protocol Version 4, Src: 10.188.226.43, Dst: 128.119.245.12**
- Transmission Control Protocol, Src Port: 58984, Dst Port: 80, Seq: 479, Ack: 1302, Len: 424**
- hyperText Transfer Protocol**

The packet details pane shows the following for the highlighted frame (Frame 1034):

```

> Frame 1034: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface en0, id 0
> Ethernet II, Src: Apple_59:c1:be (1c:57:dc:59:c1:be), Dst: Routerbo_e0:d8:16 (c4:ad:34:e0:d8:16)
> Internet Protocol Version 4, Src: 10.188.226.43, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58984, Dst Port: 80, Seq: 479, Ack: 1302, Len: 424
> hyperText Transfer Protocol

```

The packet bytes pane shows the raw hex and ASCII data for the frame.

The screenshot shows a Wireshark capture window with the following details:

- Capturing from Wi-Fi: en0**
- http** selected in the tree view.
- Frame 1057: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface en0, id 0**
- Ethernet II, Src: Apple\_59:c1:be (1c:57:dc:59:c1:be), Dst: Routerbo\_e0:d8:16 (c4:ad:34:e0:d8:16)**
- Internet Protocol Version 4, Src: 10.188.226.43, Dst: 178.79.137.164**
- Transmission Control Protocol, Src Port: 58985, Dst Port: 80, Seq: 1, Ack: 1, Len: 391**
- hyperText Transfer Protocol**

The packet details pane shows the following for the highlighted frame (Frame 1057):

```

> Frame 1057: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface en0, id 0
> Ethernet II, Src: Apple_59:c1:be (1c:57:dc:59:c1:be), Dst: Routerbo_e0:d8:16 (c4:ad:34:e0:d8:16)
> Internet Protocol Version 4, Src: 10.188.226.43, Dst: 178.79.137.164
> Transmission Control Protocol, Src Port: 58985, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
> hyperText Transfer Protocol

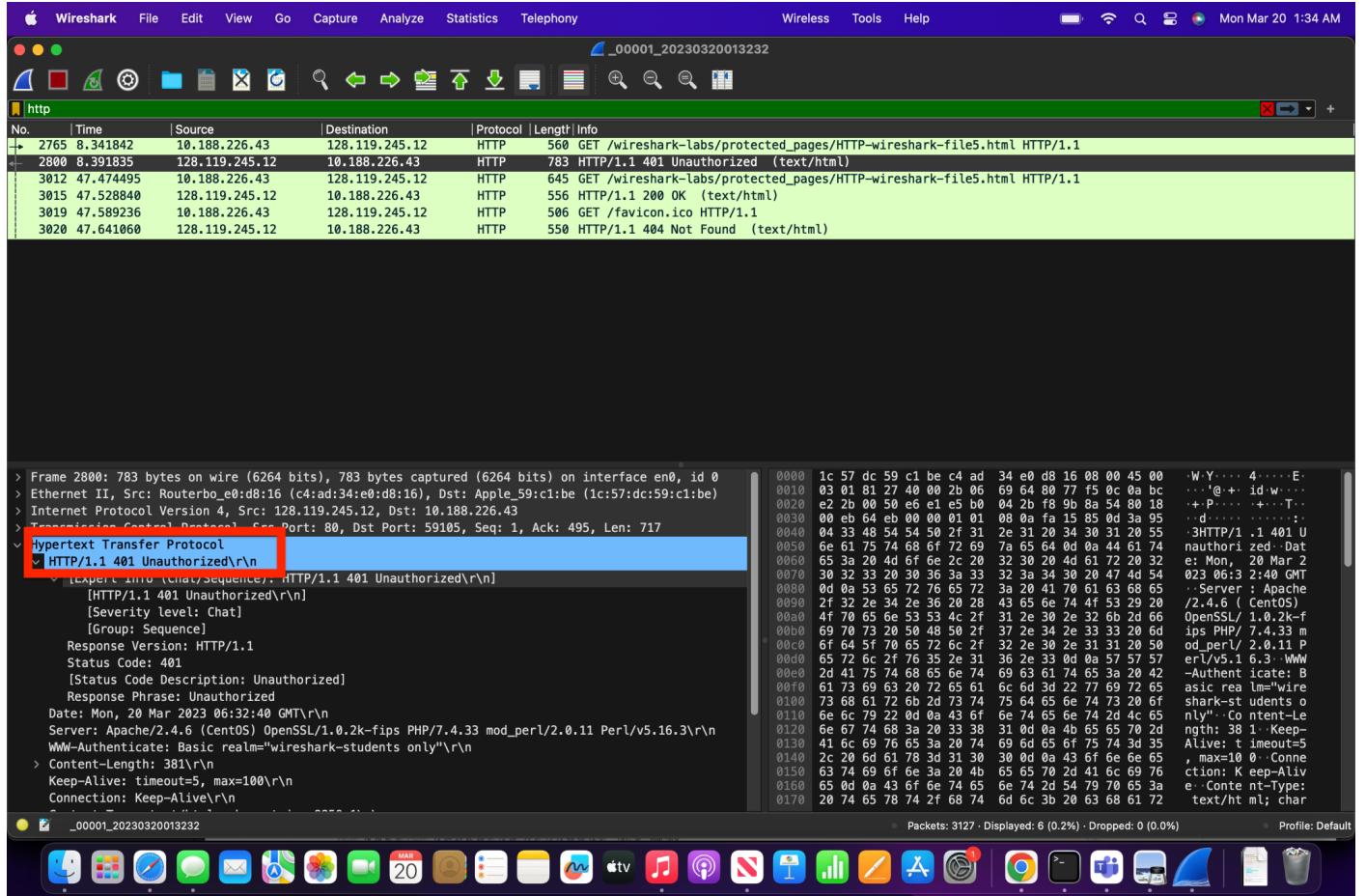
```

The packet bytes pane shows the raw hex and ASCII data for the frame.

## HTTP Authentication

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

- The server response to the initial HTTP GET request is "401 Unauthorized"



19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

- The new field in the second HTTP GET message is 'Authorization' as seen in the screenshot below.

The screenshot shows a Wireshark capture of an HTTP session. The timeline pane at the top shows several requests and responses between 10.188.226.43 and 128.119.245.12. The details pane displays the raw HTTP traffic. A specific request is selected, showing its detailed structure:

- Request Method: GET
- Request URI: /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html
- Request Version: HTTP/1.1
- Host: galia.cs.umass.edu\r\n
- Connection: keep-alive\r\n
- Authorization: Basic d2lyZXNoYXJrLXN0dWlbnRz0m5ldHdvcms=\r\n**

The Authorization header is highlighted with a red box. The bottom status bar indicates the total number of packets (3127) and bytes (6.02%) displayed.